REMARKS

Claims 1-34, 36-37, 39, 41, 43-46, 49-50, and 52-72 stand rejected under 35 U.S.C.
§ 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of
U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al. and Cavoukian
"Building in Privacy" (Cavoukian). Claims 35 and 48 stand rejected under 35 U.S.C.
§ 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of
U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and
U.S. Patent No. 6,233,618 to Herz. Claims 38 and 51 stand rejected under 35 U.S.C. § 103(a)
as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S.
Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S.
Patent No. 6,233,618 to Shannon. Claim 40 stands rejected under 35 U.S.C. § 103(a) as
being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published
Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent
No. 6,011,858 to Stock et al. Claims 42 and 47 stand rejected under 35 U.S.C. § 103(a) as
being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published
Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent
No. 6,119,096 to Mann et al.

Reconsideration is requested. No new matter is added. The rejections are traversed.
Claims 73-100 are added. Claims 1-100 remain in the case for consideration.

The Applicant thanks the Examiner for clarifying the patent number of Herz, and for
pointing out the typographical error in claim 63. The Applicant also thanks the Examiner for
not making the Office Action dated May 10, 2005 final, thereby extending the Applicant the
opportunity to make further arguments and amendments at this time.

Docket No. 8514-025   Page 23 of 34   Application No. 09/398,914

PAGE 26/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52

REQUEST FOR DECLARATION OF INTERFERENCE

Applicant requests that the U.S. Patent & Trademark Office declare an interference between the present application and U.S. Patent Application Serial No. 10/625,045 to Robinson, published as U.S. Patent Application Publication No. 2004/0153421, published August 5, 2004 (the '045 application).

A. PROPOSED COUNT

In accordance with 37 C.F.R. § 41.202(a)(2), the Applicant proposes the following count:

1.   A method for providing approval of an age-restricted transaction conducted by an age presenter, comprising:

receiving, at an unattended age verification station, at least one biometric sample proffered by the age presenter via a biometric identification device;

sending the at least one biometric sample to at least one database, wherein the at least one database has at least one biometric record stored therein, wherein the at least one biometric record contains a reference of the age presenter's age;

comparing, at the at least one database, the at least one biometric sample to the at least one biometric record stored in the at least one database;

making a first determination, at the at least one database, whether the at least one biometric sample matches the at least one biometric record stored in the at least one database;

in the event the at least one biometric sample matches the at least one biometric record stored in the at least one database, making a second determination whether the age presenter's age information in the reference meets at least one system parameter;

in the event that the age mapped to the biometric record meets the at least one system parameter, approving the age-restricted transaction at the at least one database; and

receiving, at the unattended age verification station, confirmation of the age-restricted transaction approval.

2.   A method for enrolling a system user in a transaction system comprising:

providing at least one unattended age verification station, wherein the least one unattended age verification station is configured to access at least one database, wherein the at least one database has at least one biometric record stored therein, wherein the at least one

biometric record is associated with the system user and contains a reference of the age presenter's age;

    prompting the system user to proffer an enrollment data comprising age information, personal information, and at least one biometric samples;

    transmitting to the at least one database the enrollment data; and

    storing in the at least one database the enrollment data.

B. CLAIMS CORRESPONDING TO THE PROPOSED COUNT

    In accordance with 37 C.F.R. § 41.202(a)(2), applicant identifies the following claims corresponding to the proposed counts: at least claim 1 of the '045 application and at least claim 73 of the present application. These claims each correspond exactly to Count 1. Claims 86 and 91 of the patent application are narrower versions of claim 73. Claim 75 of the '045 application and at least claim 92 of the present application each correspond exactly to Count 2.

    The claim chart attached as Appendix I applies the terms of claim 73 above to the disclosure of this application as required by 37 C.F.R. § 41.202(a)(3), (a)(5), and/or (a)(6). The notation *App.* __, __, as used in Appendix I, refers to the present application followed by a page and line number. Claim 73 is supported as indicated in Appendix I, among other places. Count 1 is copied verbatim from claim 1 of the '045 application, and is identical to claim 73.

    The claim chart attached as Appendix II applies the terms of claim 92 above to the disclosure of this application as required by 37 C.F.R. § 41.202(a)(3), (a)(5), and/or (a)(6). The notation *App.* __, __, as used in Appendix II, refers to the present application followed by a page and line number. Claim 92 herein is supported as indicated in Appendix II, among other places. Count 2 is copied verbatim from claim 75 of the '045 application, and is identical to claim 92.

C. THE REQUIREMENTS OF 35 U.S.C. § 135(b) ARE MET

    The publication date of the '045 application is August 5, 2004. This application is filed herewith on August 4, 2005, less than one year after the publication of the '045 application. Accordingly, the requirements of 35 U.S.C. § 135(b)(2) are met.

Docket No. 8514-025   Page 25 of 34   Application No. 09/398,914

PAGE 28/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52

D. PRIORITY

This application was filed September 16, 1999, and is a continuation of U.S. application Serial No. 09/244,784, filed February 5, 1999, now U.S. Patent No. 6,012,039. Accordingly, the claims of this application are entitled to an effective priority date at least as early as February 5, 1999. The '045 application was filed on July 23, 2003 as a continuation-in-part of U.S. Patent Application Serial No. 10/365,239, and so has a effective priority date of July 23, 2003. Accordingly, this application has priority over the '045 application, as required under 37 C.F.R. § 41.202(a)(4). The Applicant reserves the right to establish earlier priority.

E. COPIED CLAIMS

As required by 37 C.F.R. § 41.202(a)(2), applicant identifies the following claims that are copied from the '045 application and added by the above amendment in the same sequence: 1-12, 15, 16, 18, 21, 24-25, 32, 75, 80-82, 85, 86, and 88-90.

Docket No. 8514-025   Page 26 of 34   Application No. 09/398,914

PAGE 29/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52

REJECTIONS UNDER 35 U.S.C. § 103(a)

Referring to claim 1, the invention is directed toward a method for processing electronic transactions. A user registers with an electronic identicator a registration biometric sample. The user formulates a rule module in a clearinghouse. The rule includes at least one pattern data and at least one execution command. The user is then identified by comparing a bid biometric sample against the biometric samples registered in the electronic identicator. Assuming the user is identified, a rule module of the user is invoked, to execute at least one electronic transmission.

Referring to claim 20, the invention is a system for processing electronic transactions. A biometric input apparatus is used, for providing a registration biometric sample to an electronic identicator during registration, and for providing a bid biometric sample to the electronic identicator when the user wants to execute an electronic transmission. A clearinghouse stores rule modules, combining pattern data with execution commands. An execution module invokes an execution command from a rule module, responsive to the electronic identicator indicating whether the user is successfully identified.

Referring to claim 25, the invention is a method for processing electronic transactions. Two users, a primary and a subordinate, each register biometric samples with an electronic identicator. The users also formulate rule modules, associating pattern data with execution commands. The subordinated user is then identified by the electronic identicator. Assuming the subordinated user is successfully identified, the subordinated user's rule modules are checked to see if they are subordinated to any of the primary user's rule modules. Assuming that one of the subordinated user's rule modules are subordinated to one of the primary user's rule modules, the primary user's rule modules are invoked, thereby executing an electronic transmission.

Referring to claim 54, the invention is a method for processing electronic transactions. A biometric sample is registered. A user-customizable rule module is formed, including at least one pattern data of the user and at least one execution command of the user. A bid biometric sample is compared with the registered biometric sample. If the comparison indicates a successful match, the rule module is invoked.

Referring to claim 63, the invention is directed toward a method for processing electronic transactions. A primary user registers a primary registration biometric sample. A secondary user registers a secondary registration biometric sample. A primary user-customizable rule module, customized to the primary user, is formed, including at least one primary pattern data of the user and at least one primary execution command of the primary

user. A secondary user-customizable rule module, customized to the secondary user, is formed, including at least one secondary pattern data of the user and at least one secondary execution command of the secondary user. The secondary rule module is subordinated to the primary rule module. A bid biometric sample taken from the secondary user is compared with at least one previously registered biometric sample. The secondary rule module is determined to be subordinated to the primary rule module. Upon a successful match, the primary rule module is invoked.

Referring to claim 64, the invention is directed toward a device for processing electronic transactions. A biometric input apparatus can provide a bid or registration biometric sample of a user. An electronic rule module clearinghouse can have at least one user-customizable rule module, including at least one pattern data of the user and at least one execution command of the user. An electronic identicator can compare a registration biometric sample with a bid biometric sample. A command execution module can execute at least one execution command.

In all of the foregoing claims, the rule modules is invoked *after* identification of the user.

In contrast to all of the foregoing claims, Bianco teaches a system for authenticating users and granting conditional access to resources. In Bianco, the user provides a user ID. The biometric group to which the user belongs is determined: the biometric policy of the biometric group controlling the authentication of the user. The user's registered biometric sample, associated with the user ID, is also determined. The user's biometric sample is compared with the registered sample. If the samples match according to the biometric policy, then the resources associated with the biometric group may be accessed by the user.

As argued in the Response to the Office Action dated May 22, 2002, there are several differences between the invention and the cited prior art. In the Interview Summary dated August 27, 2003, the Examiner indicated that some of these points were discussed. These points were, in the order mentioned by the Examiner, that identification as described in the claims "is distinct from the authorization and validation techniques of Bianco"; that the rule modules of the claims are user-customizable, whereas Bianco's rule modules are not user-customizable; and that the rules in Bianco are applied pre-authentication, whereas the rule modules of the claims are applied post-identification. In other words, the Examiner agreed with the Applicant that there were at least three points on which the claims could be distinguished over Bianco.

In rejecting the claims in the Office Action dated July 19, 2004, the Examiner has combined Bianco with two additional references: the published patent application of O'Flaherty and the Cavoukian article. The Examiner cites to O'Flaherty only to find support for the concept of users being able to customize data in a database. The Examiner's stated reason for including Cavoukian is that Cavoukian teaches biometric identification and authentication.

With reference to Cavoukian, the Applicant believes the article is self-contradictory. The Applicant acknowledges that Cavoukian describes "biometrics [as] permit[ting] authentication without identification of the user". But the Applicant is lost in understanding how biometrics could be used in this way. Biometrics are inherently unique to the individual. Thus, a biometric taken from person A will, by definition, be different from a biometric taken from person B. Thus, if person A provides the biometric, the only person the biometric should match in the database is person A, meaning that person A has been identified.

The only reasonable interpretation of Cavoukian is that the database storing the "bioscrypts" does not associate the "bioscrypt" with a person's name. But this does not mean that the person is not identified; it only means that the person's name is not directly associated with the "bioscrypt". Clearly, it would take only a trivial modification of the database to associate the person's name with the "bioscrypt".

Cavoukian goes on to recite that "the bioscrypt bears no physical resemblance to the user's actual fingerprint. [The] system does not retain any record, image or template of the individual's actual fingerprint. Therefore, a copy of the fingerprint is never kept on file." But this does not mean that the individual is not uniquely identified in the database when a match is found. This comment only means that the process is not reversible: given a "bioscrpyt", the original fingerprint cannot be derived.

To use Cavoukian's example, she describes the use of biometrics to obtain welfare benefits "anonymously". But the "anonymity" to which Cavoukian refers is not a lack of identification; it is simply denying the name of recipient to the person offering the services. Because the government would not want welfare benefits to be provided to persons not entitled, somewhere there would be a database of biometrics of each legitimate welfare recipient. Each biometric in that database matches a biometric of a person. By not including the name of the welfare recipient, the services provider is not told the *name* of the welfare recipient. But because the government limits welfare benefits, the government would want to know what benefits have been received by which recipients. Thus, the recipient is identified to the government; he is anonymous only to the services provider.

Docket No. 8514-025   Page 29 of 34   Application No. 09/398,914

To further elaborate, consider the following. If a person enters a store and says that his name is "John Smith", that name does not uniquely identify him. After all, he could be the John Smith from Los Angeles, CA, or the John Smith from Miami, FL (assuming each location has one John Smith). A name does not necessarily identify; we as a society openly state that names are unique, but when pressed will admit that names are not necessarily unique. That is why, for example, drivers' licenses have unique numbers as issued by the state: the combination of the issuing state and the license number uniquely identify the individual, in a way a name never could.

Thus Cavoukian, despite the language of her article, does not in fact accomplish what she says is her goal. And this makes sense: if an individual cannot be identified, he cannot be personally held responsible for his actions. Such anonymity is unacceptable in most endeavors in life. Thus, Cavoukian's "anonymity" is not is not true anonymity, whereby a person is never uniquely identified; her "anonymity" is only from the people to whom the identity is not relevant. Against parties that want to know the person's identity, there is no anonymity.

Finally, Cavoukian only explains the benefits of her pseudo-anonymity. She does not explain how it might be implemented. Thus, Cavoukian can at best be said to explain why one might want to implement her scheme; the article fails to enable a system that provides pseudo-anonymity. Because Cavoukian is not an enabling description, its teaching is insufficient to render the claims obvious.

In addition, as said in the Response to the Office Action of November 4, 2003, it makes no sense to provide *users* the ability to modify the biometric policies in Bianco. As stated at column 2, lines 61-63 of Bianco, "the biometric policies determine the way or method in which a user is to be authenticated by the system." In other words, the biometric policies specify how the user gains access to resources on the system. If users could modify the biometric policies, they could weaken the security associated with resource access, even to the point of not requiring any security at all. Clearly, a system that allows the user to modify the security associated with accessing a resource is no more secure than a system without any access control at all. Since security and access control are important to Bianco, it would make the Bianco system inoperative for its intended purpose, and therefore would not be obvious to give users the ability to change the security of the system, as would happen if Bianco and O'Flaherty were combined as suggested by the Examiner.

Even if the Examiner intended to analogize between the biometric groups (instead of the biometric policies) of Bianco with rule modules in the claims, the analogy still fails. As

Docket No. 8514-025   Page 30 of 34   Application No. 09/398,914

PAGE 33/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52
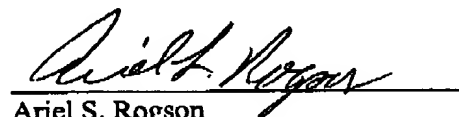
argued in the Response to the Office Action dated May 22, 2002, the biometric groups are used to determine which biometric policies to apply in authenticating the user, which means that the biometric groups are used *before* the user is authenticated, and not after the user is identified as claimed.

To summarize: the Examiner has acknowledged that Bianco fails to teach certain features of the claims. The Examiner does not cite to O'Flaherty for these concepts, and Cavoukian, aside from a being a self-contradictory document, is not enabling, and so cannot teach the missing features of the claims. The Applicant also believes the Examiner has failed to make a prima facie argument that the claims are obvious, because the Examiner has failed to present arguments that the prior art teaches biometric identification or applying the rule modules after identification. For these reasons, the Applicant believes claims 1-72 are patentable under 35 U.S.C. § 103(a) over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al. and Cavoukian "Building in Privacy" (Cavoukian) and the other references. All arguments made previously are also hereby resubmitted.

For the foregoing reasons, reconsideration and allowance of claims 1-100 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
1030 SW Morrison Street
Portland, OR 97205
503-222-3613
Customer No. 20575

APPENDIX I

73. A method for providing approval of an age-restricted transaction conducted by an age presenter, comprising:	approval = successful identification: App. 10, 29-30. age-restricted = pattern data: App. 33,3-7. transaction = authorizing and executing electronic transmissions: App. 16, 30 -OR- accessing, processing and presentation of electronic transmissions: App. 14, 16-17. age presenter = user: App. 16, 32 and App. 20, 1.
receiving, at an unattended age verification station, at least one biometric sample proffered by the age presenter via a biometric identification device;	receiving = gather(ing): App. 19, 27 and App. 20, 1 and 11. unattended age verification station = biometric input apparatus (BIA): App. 19, 27 and App. 20, 1. biometric sample = biometric sample: App. 11, 29. biometric identification device = biometric sensor: App. 20, 11-14.
sending the at least one biometric sample to at least one database, wherein the at least one database has at least one biometric record stored therein, wherein the at least one biometric record contains a reference of the age presenter's age;	sending = transmission -OR- electronic transmission of data: App. 17, 2 -OR- forwards: App. 42, 17. database = database: App. 29, 4 -OR- biometric sample database: App. 29, 8. biometric record = registered biometric sample: App. 29, 9 -OR- previously stored biometric samples: App. 27, 4. reference of the age presenter's age = user's date of birth: App. 33, 7.
comparing, at the at least one database, the at least one biometric sample to the at least one biometric record stored in the at least one database;	comparing = matching: App. 29, 8-9 -OR- comparing: App. 27, 3.
making a first determination, at the at least one database, whether the at least one biometric sample matches the at least one biometric record stored in the at least one database;	making a first determination = checking if successfully matched: App. 27, 4. matches = matched: App. 27, 5.

Docket No. 8514-025   Page 32 of 34   Application No. 09/398,914

PAGE 35/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52

in the event the at least one biometric sample matches the at least one biometric record stored in the at least one database, making a second determination whether the age presenter's age information in the reference meets at least one system parameter;	second determination = biometric comparisons with multiple biometrics: App. 29, 18. system parameter = pattern data: App. 33, 3 and App. 18, 25 -OR- multiple biometrics: App. 29, 18. age information = user's date of birth: App. 33, 7.
in the event that the age mapped to the biometric record meets the at least one system parameter, approving the age-restricted transaction at the at least one database; and	mapped = matched: App. 27, 5.
receiving, at the unattended age verification station, confirmation of the age-restricted transaction approval.	receiving = forwards to the kiosk: App. 43, 3 -OR- forwards to the BIA: App. 43, 15. confirmation of the age-restricted transaction approval = confirm to the user that the current third-party database was accessed: App. 35, 4 -OR- upon...successful identification of the user: App. 36, 9 and App. 42, 27...to purchase (age-) restricted products: App. 36, 18

Docket No. 8514-025   Page 33 of 34   Application No. 09/398,914

PAGE 36/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52

APPENDIX II

92. (New) A method for enrolling a system user in a transaction system comprising:	enrolling = registration, App. 23,6. system user = user, App. 23,6.
providing at least one unattended age verification station, wherein the least one unattended age verification station is configured to access at least one database, wherein the at least one database has at least one biometric record stored therein, wherein the at least one biometric record is associated with the system user and contains a reference of the age presenter's age;	unattended age verification station = biometric input apparatus (BIA): App. 19, 27 and App. 20, 1. database = database: App. 29, 4 - OR- biometric sample database: App. 29, 8. biometric record = registered biometric sample: App. 29, 9 -OR- previously stored biometric samples: App. 27, 4. reference of the age presenter's age = user's date of birth: App. 33, 7.
prompting the system user to proffer an enrollment data comprising age information, personal information, and at least one biometric samples;	prompting: enrollment data = App. 20,1; age information = age information = user's date of birth: App. 33, 7. personal information = App. 20,1; biometric sample database: App. 29, 8. biometric record = registered biometric sample: App. 29, 9 -OR- previously stored biometric samples: App. 27, 4.
transmitting to the at least one database the enrollment data; and	transmitting = transmission -OR- electronic transmission of data: App. 17, 2 -OR- forwards: App. 42, 17.
storing in the at least one database the enrollment data.	database = database: App. 29, 4 - OR- biometric sample database: App. 29, 8. biometric record = registered biometric sample: App. 29, 9 -OR- previously stored biometric samples: App. 27, 4. reference of the age presenter's age = user's date of birth: App. 33, 7.

Docket No. 8514-025   Page 34 of 34   Application No. 09/398,914

PAGE 37/37 * RCVD AT 8/4/2005 6:54:10 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/30 * DNIS:2738300 * CSID:5032744622 * DURATION (mm-ss):11-52